EVERY REGARD s.r.o.
Zámostní 1155/27
Ostrava-Slezská Ostrava, 710 00
IČO: 05460034 – společnost není plátcem DPH

Co je bezpečnostní incident.

1. Za zjištění narušení bezpečnosti osobních údajů se považuje situace, kdy oznamovatel (poskytovatel veřejně dostupných služeb elektronických komunikací v přímém smluvním vztahu s koncovým uživatelem) získal dostatečné informace o tom, že došlo k bezpečnostní události, která měla za následek narušení osobních údajů tak, aby podal opodstatněné oznámení o narušení bezpečnosti osobních údajů Úřadu pro ochranu osobních (dále jen oznámení Úřadu).
2. Oznámení Úřadu je nutno zaslat do 24 hodin po zjištění narušení bezpečnosti osobních údajů. Pokud oznamovatel nemá k dispozici všechny informace předkládané v oznámení Úřadu a je nutné další vyšetřování narušení bezpečnosti osobních údajů, podá do 24 hodin oznámení Úřadu vyplněné v oddíle 1 (první oznámení). Další údaje (tj. identifikační údaje a ostatní aktualizované údaje oddílu 1, pokud je aktualizace třeba, a údaje oddílu 2) podá jako změnu/doplnění oznámení o narušení bezpečnosti osobních údajů (druhé oznámení), a to nejpozději do tří dnů po podání prvního oznámení. Jestliže oznamovatel ani po vyšetřování nemůže ve lhůtě tří dnů od prvního oznámení Úřadu poskytnout všechny informace, oznámí informace, které má v této lhůtě k dispozici a předloží Úřadu pro ochranu osobních údajů odůvodnění, proč musí být zbývající informace oznámeny později. Oznamovatel co možná nejdříve oznámí zbývající informace Úřadu pro ochranu osobních údajů a v případě potřeby aktualizuje již poskytnuté údaje.
3. Oznámení Úřadu se může zasílat elektronicky (prostřednictvím datové schránky) nebo dopisem (u subjektů, které datovou schránku nemají nebo mají nastavenu pouze na příjem zpráv) v listinné podobě nebo zasláním formuláře na nosiči dat.
4. Elektronicky se oznámení Úřadu vyplňuje přímo na webových stránkách Úřadu pro ochranu osobních údajů, po vyplnění formuláře označte nabídku uložit v pdf, která vám umožní uložit vyplněný formulář na vámi zvolený datový nosič/do vámi zvoleného adresáře. V rámci ukládání je generován název souboru (na základě údajů vložených uživatelem). Název souboru nesmí být z technických a organizačních důvodů měněn – umožňuje identifikovat oznamovatele, datum podání a druh oznámení. Výsledný soubor připojte jako přílohu k datové zprávě a odešlete do datové schránky Úřadu pro ochranu osobních údajů: **qkbaa2n**.
5. V případě využití listinné podoby vytiskněte formulář, oznámení vyplňte (případně v elektronické podobě uložte na nosič dat) a poštou zašlete na adresu Úřadu pro ochranu osobních údajů: Pplk. Sochora 27, 170 00 Praha 7.
6. K oznámení Úřadu nesmí být, s výjimkou vyplněného formuláře, přiloženy žádné další dokumenty obsahující osobní údaje (například seznam osob a jejich osobních údajů zasažených narušením bezpečnosti osobních údajů).

Jaké případy je třeba ohlašovat?

Je třeba ohlašovat jakékoliv porušení zabezpečení osobních údajů, které může mít za následek riziko pro práva a svobody fyzických osob.

Může jít například o útok proti počítači, ve kterém jsou osobní údaje zpracovávány, jehož důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití. Může jít také např. o ztrátu listinných dokumentů obsahujících osobní údaje, které byly součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byly vytištěny z

počítače, ve kterém je taková evidence vedena a obsah těchto dokumentů zakládá riziko pro dotčené osoby (např. ztráta zdravotnické dokumentace).

Jaké případy není třeba ohlašovat?

Ohlašovat není třeba případy, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby.

Může jít např. o momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené evidence (kartotéky) fyzických osob nebo byl vytištěn z počítače, ve kterém je taková evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení.

Co musí ohlášení obsahovat?

Ohlášení musí obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů (pozn.: zejména ve vztahu vůči subjektům údajů);

d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Byl-li správcem nebo zpracovatelem jmenován pověřenec, k jehož úkolům patří spolupráce s dozorovým úřadem, může být vypracování ohlášení úkolem tohoto pověřence.

Komu se ohlášení zasílá?

Správce osobních údajů ohlašuje případ dozorovému úřadu, kterým je Úřad pro ochranu osobních údajů se sídlem Pplk. Sochora 27, Praha 7.

Použít však může i elektronickou formu, kdy vyplněný formulář Ohlášení porušení zabezpečení osobních údajů dle GDPR po vyplnění a uložení zašle na e-mail: posta@uoou.cz nebo do datové schránky: qkbaa2n.

Zpracovatel ohlašuje případ příslušnému správci.

Do kdy je třeba ohlášení učinit a jak?

Správce i zpracovatel ohlašují případ bez zbytečného odkladu. Správce případ ohlásí Úřadu pokud možno do 72 hodin od okamžiku, kdy se o něm dověděl. Pokud není ohlášení Úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Správce zasílá Úřadu ohlášení na adresu elektronické pošty, e-mail: posta@uoou.cz nebo do datové schránky: qkbaa2n.

Zpracovatel zasílá ohlášení správci na dohodnuté kontaktní údaje správce.

Kdy je třeba případ oznámit lidem, u nichž k porušení zabezpečení jejich osobních údajů došlo?

Je to třeba, když je pravděpodobné, že případ bude mít za následek vysoké riziko pro práva a svobody dotčených osob.

Může jít např. o případ porušení zabezpečení osobních údajů v bankovním systému, v jehož důsledku by mohlo dojít k majetkové újmě klientů banky.

Jaké jsou výjimky z povinnosti oznámit takový případ těmto lidem?

Oznámení dotčeným osobám se nevyžaduje jestliže:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;

b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek uvedených v odstavci 3.

Mám v souvislosti s porušením zabezpečení osobních údajů povinnosti i vůči jiným orgánům?

V případě, že jste jednou z povinných osob dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, konkrétně pak správcem či provozovatelem významného informačního systému, informačního systému základní služby či informačního nebo komunikačního systému kritické informační infrastruktury a jako správce osobních údajů vyplňujete formulář pro ohlášení porušení zabezpečení osobních údajů dle GDPR, můžete mít povinnost i k hlášení kybernetického bezpečnostního incidentu vůči Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Formulář hlášení kybernetického bezpečnostního incidentu NÚKIB naleznete zde.

V případě, že jste některou z ostatních povinných osob dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, tedy poskytovatelem digitální služby nebo orgánem nebo osobou zajišťující významnou síť a jako správce osobních údajů vyplňujete formulář pro ohlášení porušení zabezpečení osobních údajů dle GDPR, můžete mít povinnost hlásit kybernetický bezpečnostní incident CSIRT.CZ. Formulář hlášení kybernetického bezpečnostního incidentu CSIRT.CZ naleznete zde.